REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 542-7800 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Interview Summary

The Applicants' representative conducted a telephonic interview with the Examiner commencing at approximately 2 PM on April 19, 2006. This interview addressed the pending rejections in this application and the Applicants' proposed amendments to certain of their claims.

As to claim 33, the Applicants suggested adding a further limitation to this claim which expressly recited that the output data remains unaffected regardless of whether masking is employed or not. Upon considering this limitation, the Examiner indicated that the claim, as so amended, would sufficiently distinguish over the applied art but might require further searching on her part.

As to claim 36, the Examiner stated, in response to the Applicants' request for clarification, that she views the limitation "predetermined properties" as recited in this claim as encompassing a condition, described in the Wood patent (USP 5,003,596) in col. 5, lines 54-58, as that of no further blocks of plaintext then being available which, when that happens, halts further encryption (system operation). The Examiner suggested that the Applicants might want to amend this limitation to adequately distinguish the properties involved from simply being successive blocks of plaintext data.

The Applicants sincerely thank the Examiner for the opportunity to have conducted the interview and for all the courtesies she extended to the Applicants' representative in connection therewith.

Claim status

Claims 33 and 34 have been amended.

Specifically, claim 33 now includes the additional limitation discussed during the interview. Claim 34 now includes the limitations of claim 35. Claim 35 has now been canceled.

No other claims have been amended or canceled. No claims have been added.

Objections

In the present action, the Examiner objected to claims 35 and 37-49 as being dependent on a rejected base claim, but stated that these claims would be allowable if appropriately re-written to include the limitations of the base claim and all intervening claims.

In response, the Applicants have now amended independent claim 34 to include the limitations of claim 35. Hence, claim 34 should now be allowable, as well as claims 56-58 which depend therefrom. Claim 35 has now been canceled.

In view of the amendment now made to claim 33, as discussed during the interview which should render this claim allowable, claims 37-52 which depend, either directly or indirectly, therefrom and claims 53-55, which reference and incorporate the limitations of claim 33, should all now be allowable.

Rejections

A. Rejections under 35 USC § 102

The Examiner has rejected claims 33 and 34 under the provisions of 35 USC § 102(b) as being anticipated by the teachings of the Wood patent (United States patent 5,003,596 issued to M. Wood on March 26, 1991).

In light of the amendments, as discussed above, now made to claims 33 and 34, this rejection is moot. These claims should now be allowable.

Consequently, the Applicants see no need to comment any further on these claims, as they currently stand.

This rejection should now be withdrawn.

B. Rejections under 35 USC § 103

1. Claim 36

The Examiner has rejected claim 36 under the provisions of 35 USC § 103 as being obvious in light of the Wood patent, as applied to claims 33 and 34 (as they stood prior to this amendment) and further in view of Schneier (B. Schneier, Chapter 15 "Combining Block Ciphers", Applied Cryptography, 2nd Ed.(© 1996), pages 366-367) (the "Schneier reference").

The Examiner, as she stated during the interview, takes the position that the Wood patent discloses the concept, as recited in claim 36, of performing the supplementary process only if the data has predetermined properties. In that regard, the Examiner cites to the Wood patent for its teachings, in col. 5, lines 54-58, of the concept of ceasing further encryption if no further blocks of plaintext data are then available for encryption, hence viewing the block-wise organization of plaintext data and,

more particularly the lack of any further such blocks for encryption, as a predetermined property.

Further, the Examiner states that the Wood patent teaches various recitations in claim 36 with exception of one, namely that data (X) is fed to a supplementary process (P*) in addition to an auxiliary key (K*). In view of this omission, the Examiner turns to the Schneier reference for its teachings of a "whitening process" in which a supplementary process is an exclusive or (XOR) combinatory process and both the data and some key material are fed to the XOR process before executing a primary process, there being DES (Data Encryption Standard). Given this, the Examiner then concludes that it would have been obvious to one of skill in the art at the time of the Applicants' invention to feed the data and a key to a supplementary XOR process in order to hide plaintext patterns, i.e., a process being similar to masking, and thus arrive at the Applicants' present invention as presently recited in claim 36.

As the Examiner will soon appreciate, this conclusion is incorrect.

For the sake of brevity, the Applicants will refrain from summarizing their present invention and the general teachings of the Wood patent, and will simply refer the Examiner back to pages 13-18 of the immediately prior preliminary amendment for that summary.

The Wood patent describes its encryption system, as shown in FIG. 1, as containing an execution loop formed

of blocks 16-20, which encrypts each block of plaintext data, on a block-by-block basis, into ciphertext until as determined by decision block 18 no more blocks of plaintext data then exist to be encrypted. Once the last such block is encrypted, then execution ceases as decision block 18 directs execution via "NO" path to stop point 22. In that regard, col. 5, lines 54-58 of the Wood patent expressly state:

> "Control then passes to reference 16 where the selected block of plaintext is encrypted in accordance with the cryptographic system of the present invention. If there is more plaintext left to be encrypted, as determined by query 18, the next block of plaintext is selected at reference 20 and the next block is encrypted. If there is no more plaintext, then the system stops operation at reference 22."

Now, even if we assume, simply for purposes of argument, that the Examiner's view of predetermined properties is correct, the operation recited in claim 36 lies directly contrary to the operations described in the above-cited portion of the Wood patent.

Specifically, when no blocks of ciphertext are left to be encrypted, the Wood patent expressly teaches that further encryption halts. This, of course, makes sense as there is then nothing further to encrypt.

Claim 36 recites:

> "A method for cryptographically processing data, comprising the steps of:
> a) feeding, to a cryptographic process (P), values of data (X) and a key (K);

b) performing the cryptographic process (P) in order to form cryptographically processed output data (Y);
c) feeding, to an supplementary process (P*), a supplementary key (K*) in order to form the key (K);
d) wherein:
the supplementary key (K*) masks the key (K) used in the process (P);
the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed;
the data (X) is also fed to the supplementary process (P*); and
the supplementary process (P*) is performed only if the data (X) has predetermined properties."

The express language of this claim requires that step b), i.e., performing a cryptographic process (P) in order to form cryptographically processed output data (Y), is undertaken regardless of whether the input, e.g., plaintext, data then has predetermined properties or not. If that data does not then possess its predetermined properties, then the supplementary process is not undertaken. However, the primary process, step b), is not so constrained. That process continues in operation. This distinction is of crucial importance.

Now, with that distinction in mind, if we accept the Examiner's view that predetermined properties are, as she concludes in light of the teachings of the Wood patent, that no more plaintext blocks exist for encryption, then, that patent explicitly requires that both encryption and system operation stop. Yet, by the express language of claim 36, step b), namely cryptographic processing, i.e., encryption, would nevertheless continue. If the Examiner is correct, then how can this be? Such operation directly contradicts the explicit teachings in the very language to

which the Examiner cited in the Wood patent, namely col. 5, lines 54-58.

According to the present invention and as recited in claim 36, the data encryption continues if the input (plaintext) data does not have predetermined properties. In the context of an example described in the present specification at page 14, line 1 et seq, these properties may illustratively be that the lowest order 2-bits of the data are zero. If the lowest order 2 bits of a plaintext block are not zero, then the supplementary process will not be executed and hence either the primary key (K) will not be generated or an incorrect key will be generated. Hence, while the encryption, step b), will still proceed, the results will be incorrect and thus complicate and frustrate any third-party cryptanalysis. It is only when the input data has certain values, here being that the lowest order 2 bits are zero, that the supplemental process is performed and the correct key (K) is then generated which, in turn, yields correctly encrypted output data. Thus, whether the output data is correctly encrypted depends on the characteristics of the input plaintext itself, i.e., whether it then possesses its predetermined properties or not.

As the Examiner can appreciate, output data is encrypted and provided through the present invention, as recited in claim 36, independent of whether the correct key (K) is produced and hence whether the supplementary process is performed or not, and ultimately whether the input data matches its predetermined properties or not.

Not only is this operation not taught, disclosed or even suggested by the teachings of the Wood patent, this operation lies directly opposite to the encryption operation which is taught.

Consequently, given the inherent contradiction between claim 36 and the teachings of the Wood patent, as interpreted by the Examiner, then, to resolve this contradiction, logic dictates that either or both of two alternatives must exist:

(a) the Examiner interpretation, that predetermined properties includes whether input data has any further blocks, is incorrect, i.e., the term "predetermined properties" excludes that interpretation; and/or

(b) contrary to the Examiner's view, step b) of this claim is not taught at all by the Wood patent as that step is performed independent of whether the input data then possesses its predetermined properties or not.

The Schneier reference, given its lack of relevant teachings, completely fails to address, let alone resolve, this inconsistency.

Specifically, the Schneier reference discloses, as the Examiner correctly notes, a "whitening process" where data and key material are combined, via an XOR operation, prior to being applied, as input, to a DES or other block encryption process. However, the Schneier reference contains no disclosure, whether explicit or even implicit, that would teach away from the concept taught by the Wood patent and cited by the Examiner, namely halting further encryption if no more plaintext data blocks exist.

Therefore, if the Examiner maintains her interpretation of "predetermined properties" as simply being a block-wise organization of input data and specifically an absence of any such blocks, then any combination of the teachings of the Wood patent and the Schneier reference would lead to the very same inconsistencies, as discussed above, which result from comparing the express language of claim 36 against the encryption operation taught by the Wood patent.

Consequently, the Applicants submit that in view of the sharp divergence in operation between the system as taught by the Wood patent, based on the Examiner's interpretation, and that required by the language of claim 36, this claim is certainly not obvious to anyone of skill in the art.

Hence, the Applicants submit that claim 36 is patentable under the provisions of 35 USC § 103.

2. Claims 51, 57 and 67

The Examiner has rejected dependent claims 51, 57 and 67 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood patent, as applied to claims 33 and 34, and taken in view of the teachings in the Miyano patent (United States patent 5,442,705 issued to H. Miyano on August 15, 1995).

Claims 51 and 57 directly depend from independent claims 33 and 34, respectfully. Given the amendments now made to independent claims 33 and 34 which render each of these claims allowable, then claims 51 and 57, each of which

recites further distinguishing features of the present invention over those recited in claims 33 and 34, are likewise allowable for the same reasons as are claims 33 and 34. Hence, this rejection is now moot with respect to claims 51 and 57.

Claim 67 merely references claim 65 which, in turn, references and incorporates the limitations of claim 36. With that in mind, this rejection will be discussed with respect to independent claim 36.

The Examiner is certainly correct in stating that the Miyano patent teaches the use of DES (Data Encryption Standard). DES, in and of itself, is a very well known cryptographic process and, in fact, has been so known since the mid-late 1970s. The Applicants certainly make no claim to the DES algorithm.

As the Applicants discussed in their prior amendments (e.g., preliminary amendment mailed October 20, 2005), the Miyano patent basically relates to a hardware arrangement for transforming plaintext into ciphertext. This patent teaches, as shown in FIG. 1 and discussed in col. 2, line 54 et seq, the use of multiple (n) stages S1-S16 wherein each state encrypts right-hand data R_n by a cipher function F_n in dependence on a key K_n. The results of each cipher function are then combined with left-hand data L_n, through an exclusive OR operation, to form right-hand data R_{n+1} for the next stage, and so forth. The left-hand data L_n produced by each stage becomes right-hand data R_{n+1} for the next stage, and so forth. The initial right- and left-hand data (R_0 and L_0) are the same and are

the results of an initial permutation 12. The final right- and left-hand data (L_{16} and R_{16}) are applied to a permutation function 13, which is the inverse of function 12, to form resulting ciphertext.

To provide added security, a different key K_n is used in each stage and renewed at each iteration. Each key is provided by key scheduling section 10 based on an initial key. As discussed in col. 2, line 65 et seq, key scheduling section 10 is supplied with an initial 64-bit key. This key is transposed by permutation PC-1 shown in Table 1 (in col. 3, lines 6-14 of the patent) which first discards 8 bits of parity and transposes the remaining 56 bits in the order indicated by the table. The resulting transposed bits are split into two halves C and D of 28-bits each. Each half is successively circularly shifted left, by a given number of shifts (as shown in Table 2), to derive each key K_n. Bit data C_n and D_n (n = 1, 2, ..., 16) are then decreased in number from 56 bits to 48 bits via permutation PC-2 shown in Table 3. The resulting 16 keys K_1-K_{16} are respectively applied to stages S1-S16 and stored within corresponding key memories M1-M16 in those stages.

The Miyano patent utterly fails to teach the Applicants' inventive concept, as discussed above, of an invertible supplementary process (P*) through which a supplementary key (K*) can be generated based on a key (K) and an auxiliary key (K'). As is the case with the Wood patent, nothing in the Miyano patent compensates its output data for any influence which the supplementary process might have on that data, let alone making

execution of the supplementary process data-dependent, i.e., dependent on whether the input data then meets certain predetermined properties.

Therefore, even if teachings of these patents were to be combined as posed by the Examiner, the resulting combination, would still fall far short of the present invention as recited in independent claim 36.

There are simply no teachings whatsoever in either the Wood or the Miyano patents that when combined, would show, disclose or suggest -- whether expressly or even implicitly, the distinguishing features of the invention recited in that independent claim to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, independent claim 36 is not rendered obvious by the teachings of the Wood and Miyano patents whether taken singly or in any combination, including that proposed by the Examiner. Therefore, this independent claim is patentable under 35 USC § 103.

As such, claim 67, which references and incorporates the limitations of claim 36, is similarly patentable under the provisions of 35 USC § 103.

3. Claims 50, 53-56, 59-61 and 66-67

The Examiner has rejected dependent claims 50, 53-56 and 59-61 and 66-67 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood

patent, as applied to claims 33 and 34, taken in view of those in the Bouricius et al patent (United States patent 4,302,810 issued to W. G. Bouricius et al on November 24, 1981).

Each of claims 50 and 53-55, and 56 and 59-61 directly depends from, or references and incorporates the limitations of independent claim 33 or 34. Given the amendments now made to claims 33 and 34 which render each of these independent claims allowable, then claims 50 and 53-55, 56 and 59-61, each of which recites further distinguishing features of the present invention over those cited in claim 33 or 34, are likewise allowable as well for the same reasons as are claims 33 and 34. Hence, this rejection is now moot with respect to claims 50, 53-55, 56 and 59-61. Each of claims 66 and 67 merely references claim 65 which, in turn, references and incorporates the limitations of claim 36. With that in mind, this rejection will be discussed with respect to independent claim 36.

The Examiner cites to the Bouricius et al patent for its teaching, with respect to claim 67, of a method which includes an electronic funds transfer card (col. 2, line 26 of that patent).

Hence, the Examiner concludes that one of ordinary skill in the art would modify the cryptographic process, taught by the combination of the Wood and Miyano patents, by the teachings in the Bouricius et al patent to arrive at the Applicants' invention as recited in claim 36.

While the Bouricius et al patent does indeed disclose the specific element noted by the Examiner, that element, i.e., a method using an electronic funds transfer card, has no bearing on the principal distinguishing aspects of the present invention recited in claim 36, namely a cryptographic process which includes:

a) an invertible supplementary process (P*) through which a supplementary key (K*) can be generated based on a key (K) and an auxiliary key (K');

b) compensation of the output data for any influence which the supplementary process might have on that data; and

c) data-dependent execution of the supplementary process, i.e., executing the supplementary process based on whether the input data then possesses certain predetermined properties or not.

Merely adding the teachings of the Bouricius et al patent to the teachings of the Wood and Miyano patents would simply result in combined teachings, to the same extent as would arise from combining the teachings in the latter two patents, that would still fall far short of the invention as recited in independent claim 36.

There are simply no teachings whatsoever in the Bouricius et al patent that would provide let alone just suggest the presently inventive teachings which are missing from the Wood and Miyano patents to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, this independent claim is not rendered obvious by the teachings of the Wood, Miyano and Bouricius et al patents whether taken singly or in any combination, including that proposed by the Examiner. Therefore, this independent claim is patentable under 35 USC § 103.

As such, each of claims 66 and 67, which references and incorporates the limitations of claim 36, is similarly patentable under the provisions of 35 USC § 103.

4. Claims 31 and 32

Lastly, the Examiner has rejected dependent claims 31 and 32 under the provisions of 35 USC § 103 as being obvious over the teachings in the Wood patent taken in view of those in the Miyano patent as applied to claims 22 and 27 and further in view of the Heer et al patent (United States patent 6,028,933 issued to D. N. Heer et al on February 22, 2000).

Claims 22, 27, 31 and 32 have all been canceled by the Applicants' immediately prior preliminary amendment mailed October 20, 2005. The corresponding substitute claims, presented by that preliminary amendment, are 51, 57, 63 and 64, respectively.

In the same section of the present office action (section 5 on page 8) that provides this rejection, the Examiner references claims 51, 58, 63 and 64 rather than claims 22, 27, 31 and 32. The Applicants can only assume that the Examiner intended this rejection to address the former group of claims, rather than the latter; hence, the

Applicants will direct their comments accordingly. If the Applicants are mistaken in their view, then the Applicants kindly request that the Examiner advise the Applicants accordingly and specify the proper claims to which this particular rejection applies so that the Applicants can appropriately respond.

Claims 51 and 58 directly or indirectly depend from independent claims 33 and 34, respectively. Given the amendments now made to claims 33 and 34 which render each of these independent claims allowable, then claims 51 and 58, each of which recites further distinguishing features of the present invention over those recited in claim 33 or 34, are likewise allowable as well for the same reasons as are claims 33 and 34. Hence, this rejection is now moot with respect to claims 51 and 58. Each of claims 63 and 64 directly or indirectly depends from claim 36 and recites further distinguishing features over those recited in claim 36. Consequently, this rejection will be discussed with respect to independent claim 36.

The Examiner cites to the Heer et al patent for its teachings, expressed in col. 2, lines 62-67 thereof, of the use of triple DES in a cryptographic process. Hence, the Examiner concludes that one of ordinary skill in the art would modify the cryptographic process, taught by the combination of the Wood and Miyano patents, by the teachings in the Heer et al patent to arrive at the Applicants' invention as recited in claim 36.

The Heer et al patent does indeed disclose using triple DES in a cryptographic system. However, that is

irrelevant to the principal distinguishing aspects of the present invention recited in claim 36, namely:

a) an invertible supplementary process (P*) through which a supplementary key (K*) can be generated based on a key (K) and an auxiliary key (K');

b) compensation of the output data for any influence which the supplementary process might have on that data; and

c) data-dependent execution of the supplementary process, i.e., executing the supplementary process based on whether the input data then meets certain predetermined properties or not.

Merely adding the teachings of the Heer et al patent to the teachings of the Wood and Miyano patents would simply result in combined teachings, to the same extent as would arise from combining the teachings in the latter two patents, that would still fall far short of the invention as recited in independent claim 36. There are simply no teachings whatsoever in the Heer et al patent that would provide let alone just suggest the presently inventive teachings which are missing from the Wood and Miyano patents to a person of ordinary skill in the art, or motivate that person to think in a direction towards those teachings.

Hence, independent claim 36 is not rendered obvious by the teachings of the Wood, Miyano and Heer et al patents whether taken singly or in any combination, including that proposed by the Examiner. Therefore, that claim is patentable under 35 USC § 103.

As such, each of claims 63 and 64, which directly or indirectly depends from claim 36, is similarly patentable under the provisions of 35 USC § 103.

Conclusion

Thus, the Applicants submit that none of the claims, presently in the application, is anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103.

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

June 23, 2006

Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 542-7800

MICHAELSON & ASSOCIATES
Counselors at Law
P.O. Box 8489
Red Bank, New Jersey 07701-8489

CERTIFICATE OF MAILING under 37 C.F.R. 1.8(a)

I hereby certify that this correspondence is being deposited on **June 26, 2006** with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to the Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature

30,090
Reg. No.

(PTT111RCEAMEND(062306)/ca:Sitka)